УДК 004.42+004.75

МЕДИЦИНСКИЙ ЦИФРОВОЙ ПАСПОРТ, ОСНОВАННЫЙ НА ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

А. М. Плискин[1], А. Ф. Хасьянов[2]

Высшая школа информационных технологий и интеллектуальных систем Казанского (Приволжского) федерального университета

alexnetmore@gmail.com[1], ak@it.kfu.ru[2]

Аннотация

Представлена реализация медицинского цифрового паспорта, использующая технологию распределенного реестра для хранения зашифрованных медицинских данных, цифровых сущностей пациентов и медицинских работников и доступов к данным. Описана система безопасного распределенного хранения высокочувствительных конфиденциальных медицинских данных.

***Ключевые слова**: медицинские записи, электронные данные о здоровье, блокчейн, распределенный реестр, пиринговая система, IPFS, Ehtereum, Bitcoin, смарт-контракт, цифровая сущность, шифрование с открытым ключом, симметричное шифрование*

ВВЕДЕНИЕ

Медицинские данные пациентов –- высокочувствительная конфиденциальная личная информация пациента, которая всегда должна быть доступна по его требованию. При этом пациент должен видеть любое их изменение, и только он может решать, кому предоставлять к ним доступ, а кому нет.

Стандартные решения в виде централизованных узлов и баз данных имеют следующие уязвимости:

- политику доступа пациентов к своим медицинским данным определяет владелец централизованных баз данных; по сути, пациент не владеет своими данными;
- в случае взлома одного узла злоумышленники получают доступ к данным многих пользователей;

- в случае выхода из строя узла медицинские данные всех пациентов теряются и не могут быть восстановлены, если не существует их резервной копии;
- злоумышленник, имея доступ к данным, может внести в них непоправимые и не всегда заметные изменения, в результате чего медицинские данные станут недействительными, и их дальнейшее использование может привести к назначению врачом неверного лечения пациенту, что может навредить его здоровью.

Технология блокчейн [1] предоставляет распределенную, неизменяемую и прозрачную историю всех транзакций, что в свою очередь позволяет решить проблему безопасного распределенного хранения электронных медицинских записей, созданных верифицированными медицинскими работниками.

Для безопасного хранения большого количества медицинских данных, где каждый пациент имеет прямой доступ к своим данным, а сами записи может внести только верифицированный медик, необходимо решение, основанное на технологии распределенных реестров или просто блокчейн и офф-чейн пиринговых систем. Эти технологии позволяют пользователям надежно и открыто хранить любую информацию.

Целью работы является создание системы медицинского цифрового паспорта – системы для хранения конфиденциальных медицинских данных в распределенном реестре на основе технологии блокчейн и пиринговых оф-чейн решений с открытым исходным кодом.

Для реализации решения были поставлены следующие задачи:

- Разработка логики смарт-контракта в блокчейн-сети Ethereum [3] для описания и хранения цифровых сущностей пользователей системы.
- Разработка логики смарт-контракта для хранения и предоставления доступа к чтению и изменению медицинских данных пациентов для медиков.
- Разработка пользовательского приложения для загрузки данных в распределенную файловую систему IPFS [4] и блокчейн-сеть Ethereum [2].
- Разработка функционала пользовательского приложения для шифрования и дешифрования данных, а также для просмотра этой информации пользователями системы.

ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ

Следующие решения для хранения медицинских историй используют технологию распределенного реестра:

GemHealth

Эта система построена на блокчейн-платформе Ethereum. Рассматриваются кейсы для хранения информации о рецептах, посещениях и анализа медицинских данных [5]. К недостаткам системы можно отнести следующее: записи хранятся в памяти смарт-контрактов; за это необходимо платить «gas», а размеры медицинских записей могут быть большими, поэтому придется платить много «gas». Также отсутствует информация о том, в каком виде хранятся записи, шифруются ли они. Единственным владельцем медицинских данных должен быть пациент, к которому они относятся, только он может решать, кому предоставлять к ним доступ. Если данные будут находиться в открытом доступе и не будут зашифрованы, то воспользоваться ими сможет любой без разрешения пациента, к которому они относятся.

GemHealth не является проектом с открытым исходным кодом. Техническое описание распределенной системы должно быть доступно любому ее пользователю, который может удостовериться в том, что его данные действительно надежно хранятся в зашифрованном виде и никто не может без его решения получить к ним доступ. Приложение должно иметь полностью открытый исходный код; оно должно работать автономно без внешнего контроля. Приложение может адаптировать свой протокол в ответ на предлагаемые улучшения и отзывы на рынке, но все изменения должны решаться на основе консенсуса его пользователей.

MedRec

Эта система построена на блокчейн-платформе Ethereum и представляет собой журнал медицинских записей пациентов, доступ к которому можно легко дать поставщикам медицинских услуг [6]. К достоинствам системы следует отнести то, что в памяти смарт-контрактов хранятся не сами записи, а указатели на эти файлы, таким образом, снижается стоимость «gas» за хранение этих записей. К недостаткам системы можно отнести следующее: записи хранятся на базе провайдера, который оказывает медицинские услуги. При изменении данных мож-

но будет узнать о том, что они были изменены, но восстановить их в случае потери оригинала уже будет нельзя. Также решение не является полностью распределенным, поскольку при отключении провайдера от сети данные уже нельзя будет получить. Также данное решение не является проектом с открытым исходным кодом.

Blockchain Health co

Информация об этом проекте есть только на официальном сайте [7], на котором сказано, что у каждого участника есть своя цифровая сущность. Пользователи могут делиться информацией с учеными, а те в свою очередь могут использовать ее для своих исследований. Система служит для создания доступного для исследований хранилища медицинских данных. К недостаткам системы можно отнести следующее: неизвестно, где и в каком виде хранятся сами данные, также система не является проектом с открытым исходным кодом.

DokChain

Эта система представляет собой приватную блокчейн-сеть для хранения медицинских записей [8]. Данные о медицинских записях хранятся в пиринговой файловой системе IPFS, что позволяет меньше загружать блокчейн-сеть. Недостатки системы заключаются в том, что в системе используется отдельная самописная блокчейн-сеть. Неизвестны ее возможности и характеристики. Нет информации о том, функционирует ли она на уровне продукта промышленного качества. Система не является проектом с открытым исходным кодом.

e-Health Records – e-Estonia

Это эстонская национальная система для хранения медицинских данных граждан страны, которая хранит данные о 97% граждан Эстонии [9]. Пациенты в любой момент времени могут получить доступ к своим медицинским записям и просмотреть список медиков, у которых есть доступ к данным. Данные, находящиеся в блокчейн-сети, используются для статистических исследований. Главным недостатком системы является то, что она доступна только для граждан Эстонии, так как только у них есть зарегистрированная в ней цифровая сущность. Также отсутствует техническое описания работы системы, и система не является проектом с открытым исходным кодом.

Blockchain For Health Data

Стоит сразу отметить, что описан лишь концепт системы для хранения электронных медицинских карточек пациентов, но реализация отсутствует. Сведения о медицинских данных хранятся в «озере данных» (англ. data lake), а не в блокчейне [10]. Планируется публикация исходных кодов проекта. К недостаткам стоит отнести то, что представлен лишь концепт системы. Также система не является полностью распределенной, так как для хранения статических файлов используется «озеро данных», которое хранится на одном узле или группе узлов, что представляет собой кластер, доступный исключительно его владельцу. Нет информации о том, какая блокчейн-сеть будет использована, поэтому неизвестно, насколько безопасно будут осуществлены хранение цифровых сущностей и доступ к данным внутри системы.

КОНЦЕПТУАЛЬНОЕ ОПИСАНИЕ И АРХИТЕКТУРА СИСТЕМЫ

Система медицинского цифрового паспорта на основе технологии распределенных реестров представляет собой комплекс, в котором данные о пациентах, медицинских работниках и доступ к медицинским записям хранятся в памяти смарт-контракта в блокчейн-сети Ethereum. Сами записи в зашифрованном виде хранятся в распределенной файловой системе IPFS.

Любой пациент может зарегистрироваться в системе и дать разрешение медицинскому работнику на просмотр его медицинских данных и внесение новых. Сущность медицинского работника должна быть подтверждена владельцем смарт-контракта. Медик может проверить, есть ли у него доступ к записям пациента. Если доступ есть, то он может просматривать данные пациента и добавлять новые, в противном случае он не имеет доступа к данным.

Каждая медицинская запись может измеряться произвольным количеством байт. В целях уменьшения стоимости, которую приходится платить за хранение одной записи, в памяти смарт-контракта медицинская запись, предварительно зашифрованная псевдослучайным ключом, сохраняется в распределенной файловой системе IPFS. В блокчейн сохраняется адрес этого файла, который представляет собой его хэш. К самому зашифрованному файлу доступ имеет любой участник сети IPFS, при этом он представляет собой произвольный набор байт, который не несет никакой полезной информации. Благодаря этому сохра-

няется полная конфиденциальность любой медицинской записи, хранящейся в IPFS.

Любая медицинская запись шифруется симметрично алгоритмом AES [14]. В процессе регистрации в системе пользовательское приложение пациента генерирует псевдослучайный ключ, который представляет собой конкатенацию адреса из 64 произвольных битов. Сам ключ, только уже ассиметрично зашифрованный публичным ключом пациента, лежит в профиле пациента в памяти смарт-контракта. Когда пациент дает доктору доступ к своим записям, ключ для шифрования записей достается пользовательской программой пациента, расшифровывается его приватным ключом, после шифруется публичным ключом медицинского работника и сохраняется в блокчейн, добавляя новое значение в список доступов.

Система состоит из трех компонентов (Рис. 1):

1. Пользовательский интерфейс, созданный при помощи javascript-фреймворка React-Redux, библиотеки для работы с блокчейн-сетью Ethereum – web3.js, библиотеки, предоставляющий API для работы с IPFS, и библиотеки bitcore-lib.js для шифрования с открытым ключом.
2. Блокчейн-составляющая – смарт-контракт, написанный на языке Solidity [11].
3. IPFS-демон, развернутый на устройстве пользователя для взаимодействия с сетью IPFS.

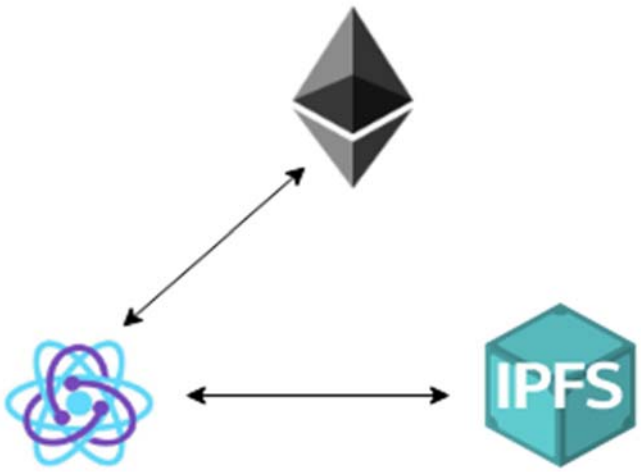

Рис. 1. Архитектура компонентов системы

СТРУКТУРА СМАРТ-КОНТРАКТА

Смарт-контракт написан на языке Solidity версии 0.4.20. Для выделения владельца смарт-контракта наследуется другой смарт-контракт Ownable, являющийся стандартом от Zeppelin [12] для наделения смарт-контракта правами собственности:

```
pragma solidity ^0.4.20;

import './Ownable.sol';

contract MedCard is Ownable {
```

Для привязки цифровой сущности медицинского работника и пациента к конкретному адресу введены словари, в которых каждому адресу соответствует структура, описывающая сущность медика и пациента:

```
mapping (address => Doctor) public doctors;

mapping (address => Patient) public patients;
```

Для составления медицинской истории пациента список адресов (хешей) медицинских записей привязан к конкретному адресу пациента:

```
mapping (address => string[]) private records;
```

Для проверки состояния пользователя в системе используются модификаторы доступа: является или нет пользователь медицинским работником; является или нет пользователь медицинским работником; является или нет пользователь пациентом:

```
modifier isDoctor(address _address) {
  ...
}

modifier isNotDoctor(address _address) {
    ...
}

modifier isPatient(address _address) {
    ...
}

modifier isNotPatient(address _address) {
    ...
}
```

В описании цифровой сущности медицинского работника хранятся хэш его профиля в IPFS, статус и публичный ключ. Статус медицинского работника может находиться в двух состояния (подтвержден и не подтвержден):

```
struct Doctor {
    string profile;
    bool accepted;
    string publicKey;
}
```

В описании цифровой сущности пациента хранятся хэш его зашифрованного профиля IPFS, зашифрованный ключ для работы с записями пациента, хэш файла с доступами для медиков и публичный ключ. В данном случае ключ шифруется публичным ключом пациента, поэтому прочитать его может только сам пациент, используя для дешифрования свой приватный ключ:

```
struct Patient {
    string profile;
    string passphrase;
    string permissions;
    string publicKey;
}
```

Для создания сущности пациента и медицинского работника добавлены соответствующие методы. Методы могут быть вызваны, если в системе пользователь не является ни пациентом, ни медиком:

```
function applyPatient(
    string _profile,
    string _passphrase,
    uint _permissions,
    string _publicKey
)
    public isNotPatient(msg.sender)
{
    patients[msg.sender] = Patient({
        profile: _profile,
        passphrase: _passphrase,
        permissions: _permissions,
```

```
            publicKey: _publicKey
        });
    }

    function applyDoctor(
        string _profile,
        string _publicKey
    )
        public isNotDoctor(msg.sender)
    {
        doctors[msg.sender] = Doctor({
            profile: _profile,
            accepted: false,
            publicKey: _publicKey
        });
    }
```

Для подтверждения статуса медицинского работника добавлен метод, который может вызвать только владелец смарт-контракта:

```
    function approveDoctor(
        address _address
    )
        public isNotDoctor(_address) onlyOwner
    {
        doctors[_address].accepted = true;
    }
```

Метод для добавления новой записи (добавляются не само содержание записи, а ее хэш из сети IPFS). Запись должна соответствовать sha3-хэшу ключа пациента для работы с записями, а добавить ее может только верифицированный доктор:

```
    function addRecord(
        string _hash,
        string _value
    )
        public isDoctor(msg.sender)
    {
        records[_hash].push(_value);
```

```
}
```

Для получения хэшей медицинских записей пациента добавлены два метода. Первый получает количество записей, второй достает хэш по индексу:

```
function getPatientRecordsLength(
    string _hash
)
    public constant returns (uint)
{
    return records[_hash].length;
}


function getPatientRecord(
    string _hash,
    uint _index)
public constant returns (string)
{
    return records[_hash][_index];
}
```

Пациент может дать доступ медикам, обновив список доступов:

```
function updatePermissions (
    string _permissions
)
    public isPatient(_msg.sender)
{
    patients[msg.sender].permissions = _permissions;
}
```

ПОЛЬЗОВАТЕЛЬСКОЕ ПРИЛОЖЕНИЕ

Пользователи системы напрямую не работают с блокчейн-сетью Ethereum. Вместо этого создано пользовательское приложение, которое дает возможность пользоваться всей бизнес-логикой смарт-контракта, шифровать и дешифровать данные о ключах и самих медицинских записях и сохранять их в IPFS.

Сначала пользователю необходимо предоставить системе доступ к своей цифровой сущности, которую определяет приватный ключ. При входе в систему пользователю предлагается выбрать файл, в котором находится приватный ключ. Сам файл должен быть формата json и выглядеть следующим образом:

```
{
    "pkey": "0x9df1b091b86983ebbfaee3613bfabf26aa873d82485c3ece4e95bc39713d8c45"
}
```

По приватному ключу система определяет пользователя и интерфейс для работы с блокчейн-сетью Ethereum.

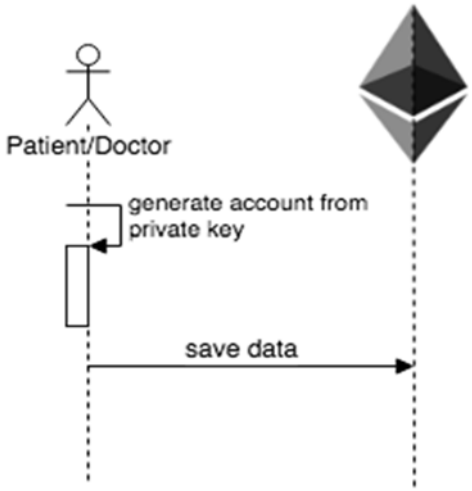

Рис. 2. Схема регистрации в системе

Если пользователь не зарегистрирован в системе, то ему предлагаются две формы для регистрации: как медицинского работника или пациента. После заполнения формы транзакция с данными отправляется в блокчейн-сеть Ethereum и сохраняется в памяти смарт-контракта (Рис. 2). Если регистрируется пациент, то для него генерируется псевдослучайный ключ, который шифруется его приватным ключом. Зашифрованный ключ также отправляется вместе с данными транзакции. После подтверждения транзакции пользователь может войти в систему, предоставив ей файл с приватным ключом. Интерфейс будет зависеть от роли пользователя.

Пациент сможет по адресу найти любого медицинского работника, дать ему доступ к своим данным. Также пациент сможет просмотреть свои медицинские записи.

Если пациент хочет дать доступ медику, то у него локально дешифруется его псевдо-рандомный ключ, который лежит в памяти смарт-контракта. Полученное значение шифруется публичным ключом медицинского работника и отправляется в память смарт-контракта (Рис. 3). В итоге у медика появляется доступ на чтение данных пользователя.

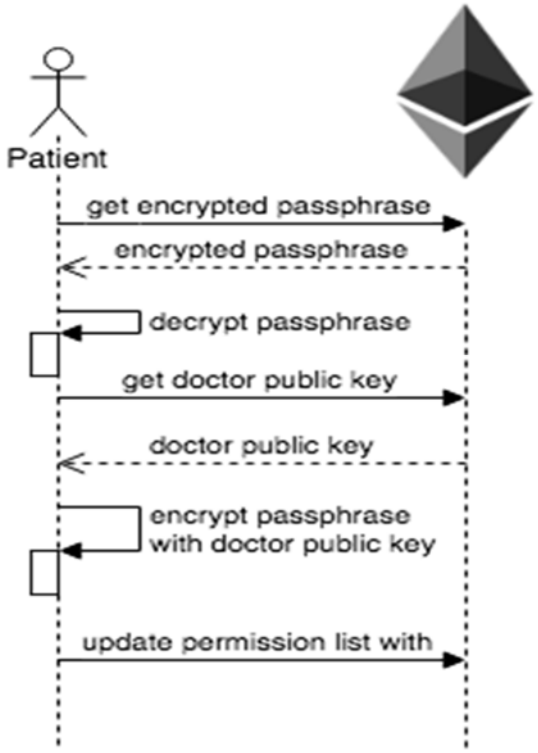

Рис. 3. Схема предоставления доступа к записям

Медицинский работник может по адресу найти любого пациента. Если у медика есть доступ, то он сможет просмотреть все записи пациента (Рис. 4) и добавить новые.

При добавлении новой записи происходит следующее: медик прикрепляет файл с новой медицинской записью; она шифруется ключом, полученным дешифрированием значения ключа конкретного пациента (ключ дешифруется приватным ключом медика) (Рис. 5). После полученный набор байт кладется в пиринговую сеть IPFS, возвращается хэш этой записи и сам хэш уже посылается транзакцией в блокчейн-сеть Ethereum.

На данном этапе разработки приложения владелец смарт-контракта может подтвердить любого медика, используя среду для написания, развёртывания и тестирования смарт-контрактов Remix.

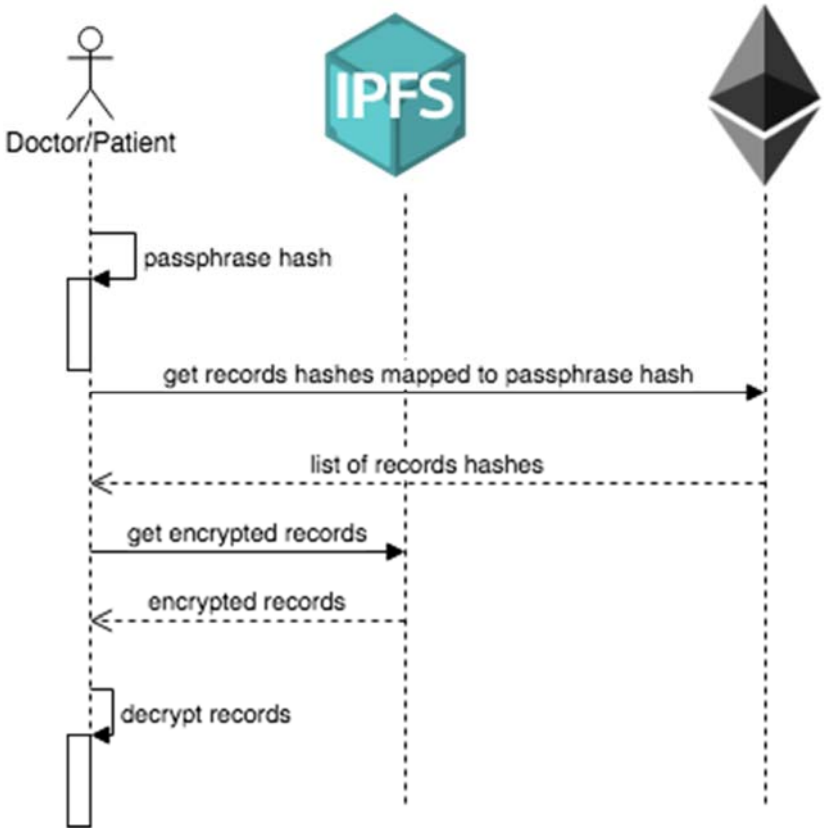

Рис. 4. Схема получения записей

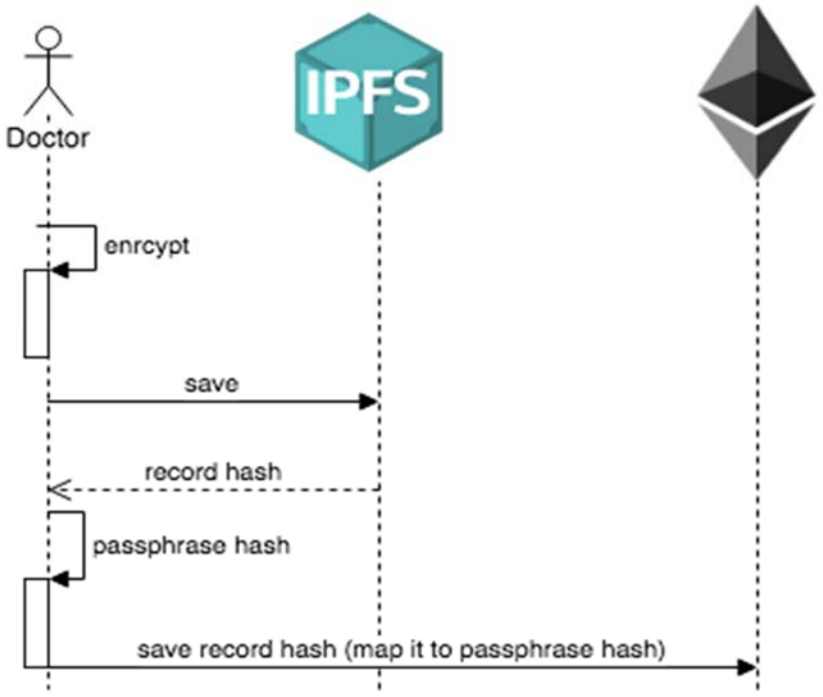

Рис. 5. Схема добавления новых записей

ЗАКЛЮЧЕНИЕ

Спроектирована, разработана и описана система для распределенного безопасного хранения медицинского паспорта пациента и обеспечения безопасного доступа к высокочувствительным медицинским записям с открытым исходным кодом, который доступен в репозитории на гитхабе (англ. github) [13]. Разработанная система имеет следующие достоинства:

- относительно невысока стоимость хранения данных в памяти смарт-контракта за счет хранения контента медицинских записей в бесплатной пиринговой сети IPFS;
- использовано асимметричное шифрование медицинских записей, которое не позволяет злоумышленникам получить доступ к конфиденциальным данным; сложность подбора закрытого ключа несоизмеримо высока и требует полного перебора всех возможных значений;

Дальнейшая работа предполагает:

- исследовать методы для верификации цифровой сущности медицинского работника; рассмотреть проекты, созданные на основе технологии

распределенных реестров, на основе которых можно получить информацию о компетенциях, лицензиях и опыте медиков;

- внести функционал в пользовательское приложение для поиска пациента и медицинского работника по QR-коду;
- добавить возможность для пациента давать доступ только к части своих данных;
- внедрить систему в инфраструктуру медицинской клиники Казанского федерального университета.

СПИСОК ЛИТЕРАТУРЫ

1. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system. 2008.
2. *Wood G.* Ethereum: A Secure Decentralised Generalised Transaction Ledger //Ethereum Project Yellow Paper. 2014. V. 151. P. 1–32.
3. *Buterin V.* Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. URL: https://github.com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper. 2014
4. *Benet J.* Ipfs-content Addressed, Versioned, p2p file system //arXiv preprint arXiv:1407.3561. 2014.
5. *Prisco G.* The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab. URL: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938
6. *Ekblaw A. et al.* A Case Study for Blockchain in Healthcare: “MedRec” Prototype for Electronic Health Records and Medical Research Data //Proceedings of IEEE Open & Big Data Conference. 2016. V. 13. P. 13.
7. Blockchain Health. URL: https://blockchainhealth.co/
8. Dockchain. URL: https://dokchain.com/download/whitepaper/
9. E-estonia healthcare. URL: https://e-estonia.com/solutions/healthcare/
10. *Linn L. A., Koo M. B.* Blockchain for Health Data and its Potential Use in Health It and Health Care Related Research //ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, United States: ONC/NIST. 2016.
11. *Dannen C.* Introducing Ethereum and Solidity. Apress, 2017.

12. Zeppelin Solidity. URL: http://zeppelin-solidity.readthedocs. io/en/latest/ownable.html

13. *Pliskin Alexander*. MedicalRecords. URL: https://github.com/GoodBoy962/ MedicalCards

14. *Баричев С. Г., Гончаров В. В., Серов Р. Е.* 2.4. 2. Стандарт AES. Алгоритм Rijdael. Основы современной криптографии. М.: Горячая линия–Телеком, 2002. С. 30–35.

MEDICAL DIGITAL PASSPORT BASED ON DISTRIBUTED LEDGER

A. M. Pliskin[1], **A. F. Khasyanov**[2]

Higher School of Information Technologies and Intellectual Systems at Kazan (Volga Region) Federal University

alexnetmore@gmail.com[1], ak@it.kfu.ru[2]

Abstract

The paper presents the implementation of the patient medical digital passport, using distributed ledger for storing encrypted electronic health records, patient and medic digital entities and accesses for data. A system for the secure distributed storage of highly sensitive confidential medical data is described.

Keywords*: medical data, electronic health records, blockchain, distributed ledger, peer-to-peer system, IPFS, Ehtereum, Bitcoin, smart contract, digital identity, public key encryption, symmetric encryption*

REFERENCES

1. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system. 2008.
2. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger //Ethereum Project Yellow Paper. 2014. V. 151. P. 1–32.
3. *Buterin V.* Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. URL: https://github.com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper. 2014
4. *Benet J.* Ipfs-content Addressed, Versioned, p2p file system //arXiv preprint arXiv:1407.3561. 2014.
5. *Prisco G.* The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab. URL: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938
6. *Ekblaw A. et al.* A Case Study for Blockchain in Healthcare: “MedRec” Prototype for Electronic Health Records and Medical Research Data //Proceedings of IEEE Open & Big Data Conference. 2016. V. 13. P. 13.
7. Blockchain Health. URL: https://blockchainhealth.co/
8. Dockchain. URL: https://dokchain.com/download/whitepaper/

9. E-estonia healthcare. URL: https://e-estonia.com/solutions/healthcare/

10. *Linn L. A., Koo M. B.* Blockchain for Health Data and its Potential Use in Health It and Health Care Related Research //ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, United States: ONC/NIST. 2016.

11. *Dannen C.* Introducing Ethereum and Solidity. Apress, 2017.

12. Zeppelin Solidity. URL: http://zeppelin-solidity.readthedocs.io/en/latest/ownable.html

13. *Pliskin Alexander*. MedicalRecords. URL: https://github.com/GoodBoy962/ MedicalCards

14. *Barichev S. G., Goncharov V. V., Serov R.E.* Standart AES. Algoritm Rijdael. Osnovi sovremennoi cryptografii. M.: Goryachay liniya–Telekom, 2002. S. 30–35.

СВЕДЕНИЯ ОБ АВТОРАХ

ПЛИСКИН Александр Маркович – студент Высшей школы информационных технологий и интеллектуальных систем Казанского федерального университета, разработчик программного обеспечения.

Alexander Markovich PLISKIN – student of the Higher Institute of Information Technologies and Intelligent Systems of Kazan Federal University, software engineer.

email: alexnetmore@gmail.com

ХАСЬЯНОВ Айрат Фаридович – директор Высшей школы информационных технологий и интеллектуальных систем Казанского федерального университета. Имеет степень PhD Боннского университета в области естественных наук. Сфера научных интересов лежит в области применения информационных и интеллектуальных технологий в области образования, различных отраслях информационных технологий и информатики.

Dr. Ayrat KHASYANOV obtained his PhD in Computer Science in 2005 from the University of Bonn in Germany. He serves his duty as the head of the Higher Institute for Information Technologies and Intelligent Systems at Kazan Federal University. His interests lay in the field of application of intelligent and information technology to the fields of teaching and learning, as well as various fields of information technology and computer science.

email: ak@it.kfu.ru

Материал поступил в редакцию 3 июня 2018 года